Conducta inesperada del NAT dinámico con el tráfico NON-Pattable

Contenido

Introducción

Este documento describe la conducta inesperada de la traducción de dirección de red dinámica (NAT) con el tráfico NON-Pattable en los dispositivos IOS®.

Problema

El tráfico NON-Pattable crea las mitad-entradas en la tabla de traducciones de NAT en caso del NAT dinámico. Estas entradas presentan como riesgo de seguridad puesto que trabajan para exterior-a-dentro del tráfico.

Configuración del NAT:

```
ip nat pool ATT_FIBER 10.10.10.1 10.10.10.6 netmask  255.255.255.248
ip nat inside source list GUEST_SUBNET pool ATT_FIBER overload
ip nat inside source list OFFICE_SUBNETS pool ATT_FIBER overload

ip access-list extended OFFICE_SUBNETS
 deny   ip 172.16.26.0 0.0.0.127 any
 permit ip 172.16.8.0 0.0.1.255 any

ip access-list extended GUEST_SUBNET
 permit ip 172.16.26.0 0.0.0.127 any

udp 10.10.10.1:49370    172.16.9.9:49370      192.168.1.1:53      192.168.1.1:53
udp 10.10.10.1:49535    172.16.9.9:49535      192.168.2.2:53    192.168.2.2:53
tcp 10.10.10.1:53133    172.16.9.9:53133      192.168.3.3:80     192.168.3.3:80
tcp 10.10.10.1:56311    172.16.9.9:56311      192.168.4.4:5816    192.168.4.4:5816
--- 10.10.10.1         172.16.9.9            ---                   ---
```

Las medias entradas se crean en ciertos casos donde hay una asignación del interior - > exterior o cuando el paquete se inicia desde adentro - > afuera.

Cuando configuran al router para la sobrecarga NAT (traducción de Addess del puerto (la PALMADITA)) y el tráfico NON-pattable golpea al router, las entradas del lazo NON-pattable consigue creado para este tráfico. Lleva a esta clase de entrada en la tabla NAT:

```
ip nat pool ATT_FIBER 10.10.10.1 10.10.10.6 netmask  255.255.255.248
ip nat inside source list GUEST_SUBNET pool ATT_FIBER overload
ip nat inside source list OFFICE_SUBNETS pool ATT_FIBER overload
```

```
ip access-list extended OFFICE_SUBNETS
 deny   ip 172.16.26.0 0.0.0.127 any
 permit ip 172.16.8.0 0.0.1.255 any

ip access-list extended GUEST_SUBNET
 permit ip 172.16.26.0 0.0.0.127 any

udp 10.10.10.1:49370    172.16.9.9:49370      192.168.1.1:53      192.168.1.1:53
udp 10.10.10.1:49535    172.16.9.9:49535      192.168.2.2:53    192.168.2.2:53
tcp 10.10.10.1:53133    172.16.9.9:53133      192.168.3.3:80     192.168.3.3:80
tcp 10.10.10.1:56311    172.16.9.9:56311      192.168.4.4:5816    192.168.4.4:5816
--- 10.10.10.1         172.16.9.9            ---                   ---
```

Esta entrada del lazo consume un direccionamiento entero del pool. En este ejemplo, 10.10.10.1 es un direccionamiento de un pool sobrecargado.

Eso significa que una dirección IP del Inside Local consigue el límite al IP del Outside Global que es similar al NAT estático. Debido a esto, hasta que la entrada actual consiga medida el tiempo hacia fuera, los nuevos IP Addresses del Inside Local no pueden utilizar este IP Address global. Toda la traducción creada para este lazo es traducciones 1 a 1 en vez de sobrecarga.

Solución

Para solucionar este problema, usted puede utilizar las ruta-correspondencias con el NAT dinámico. Con las ruta-correspondencias, el NAT no creará las mitad-entradas ni utilizará la sobrecarga de la interfaz en vez de la sobrecarga del pool. Los atascamientos NON-pattable no se crean en caso de la sobrecarga de la interfaz.